FORM PTO-1390
(REV. 11-2000)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER
5551

U S APPLICATION NO (If known, see 37 CFR 1 5
09/937819

INTERNATIONAL APPLICATION NO. PCT/DE00/00189	INTERNATIONAL FILING DATE 20 January 2000	PRIORITY DATE CLAIMED 29 March 1999

TITLE OF INVENTION
DEVICE AND METHOD FOR SECURE ELECTRONIC DATA TRANSMISSION

APPLICANT(S) FOR DO/EO/US
Volker PAUL; and Bertram BRESSER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (unexecuted)
10. ☒ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)). (with amended claims 1 and 12)

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:
    - Application Data Sheet

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937819	PCT/DE00/00189	5551

21. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)): Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .... $1000.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .... $860.00 International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... $710.00 International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) .... $690.00 International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 130.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	18 -20 =	0	x $18.00	$ 0.00	
Independent claims	1 -3 =	0	x $80.00	$ 0.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	$ 270.00	
TOTAL OF ABOVE CALCULATIONS =				$1,260.00	
□ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$ 0.00	
SUBTOTAL =				$1,260.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 0.00	
TOTAL NATIONAL FEE =				$1,260.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 0.00	
TOTAL FEES ENCLOSED =				$1,260.00	
				Amount to be refunded:	$
				charged:	$

a. ☒ A check in the amount of $ 1,260.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. ____________ in the amount of $ __________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-3690 . A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

BREINER & BREINER, L.L.C.
115 North Henry Street
P.O. Box 19290
Alexandria, VA 22320-0290

Date: September 28, 2001

Mary J Breiner
SIGNATURE

Mary J. Breiner
NAME

33,161
REGISTRATION NUMBER

Device and Method for Secure Electronic Data Transmission

The present invention relates to a device and a method for secure electronic transmission of data between end units that are temporarily or permanently connected to a server.

This method and this device are particlarly suited for electronic transmission of medical data.

From the legal point of view, the confidentiality of medical data has top priority. When transmitting medical data over publicly accessible networks, e.g. the internet or a compound network that is accessible from the outside, it is therefore necessary to provide security measures that ensure the best protection.

The protection mechanisms basically available for data transmission over public networks relate in particular to using cryptographic methods of encoding data. Usually standard cryptographic methods using secure exchange of keys corresponding to X.509 are employed: symmetric encoding processes, in particular for encoding large amounts of data and asymmetrical encoding processes using a so-called public key and a so-called private key, such as the common RSA.

The present invention relates to the transmission of data from one network participant (transmitter) to another (addressee or recipient) via intermediate storage on a data station respectively on a server. Although an asymmetrical encoding process using the public key of the addressee for encoding data offers a high degree of protection in the electronic transmission of data, this method cannot be used by addressees who in many cases are still unknown when the data are provided.
An example of this arises, for instance, in the field of medicine, as explained later on with reference to the preferred embodiment, when a physician gives a patient a transfer slip to

consult a colleague and he wants to send the colleague certain medical data of the patient electronically. In many cases, the identity of the colleague that the patient will seek is not known at the time.

The object of the present invention is to provide a device and a method for secure electronic transmission of data via the server of a network, wherein the addressee of the data does not need to be known at the time when the data is made available.

The object is solved with the device and the method set forth in claims 1 and 12. Advantageous embodiments and further improvements of the device and the method are the subject matter of the subclaims.

The invented device which has to be installed and operated in the network server is provided with an input unit for receiving coded data (from the transmitter) and an external key (of the recipient).
Furthermore, the device has a unit for decoding the coded data with an internal key and for renewed encoding of the data with external key. The internal key is filed in some technical manner inside the device and is not accessible from outside the device. The data encoded with the external key can be retrieved at an output.

It is a matter of course that the to-be processed data have to be encoded in such a manner that they can be decoded with the internal key. Thus, only coded data that the device can read are converted into recoded data inside the device with an external key for recoding. When a corresponding data request is made, the recoded data can be read by the holder of the external key, which was transferred to the device along with the data.

Fundamentally, the original transmitted data, i.e. for example medical data, can be decoded by the device and recoded again.

However, in a preferred application of the device, which is described later on, not the original data itself but only its key transferred in coded form is recoded with the device.

In a preferred embodiment, for decoding the coded data and for recoding the data, the device is provided with a chipcard as carrier of the internal key. This chipcard is preferably a chipcard from a certified trust center.
In another version, encoding and decoding can be partly or completely carried out directly by an active chipcard.

Another possibility is to employ a suited circuit in compliance with information, and communication service and signature laws, if need be software controlled, as a unit for encoding and decoding.

The heart of the invented solution is recoding the data or recoding a key accompanying the data, hereinafter referred to as session key, in such a manner that the data can be read by an authorized communication partner, the addressee. For this purpose, in the preferred embodiment, a session key used for symmetrical encoding of data is decoded with the private key of the server and immediately recoded with the public key of the recipient or addressee requesting the data. This key is preferably stored in the server in a list of participating and authorized network participants, e.g. along with the participant's ID and the ISDN number, and can be updated at any time as needed through the services of a trust center.

Decoding the original data per se is not necessary with this method. Required for later decoding of the data is only the session key, now readable for the recipient, which was generated for instance by chance during encoding as explained in more detail in the preferred embodiment.

In this way, it is avoided that the data are ever in the server uncoded. In detail this means that there is no access to the coded data during the recoding processes at all. Processed is only the session key used for their encoding which was "recoded" in a closed process from a form that only the server respectively the invented device installed in the server can read into a form that the requester can read.

Application of the device is made more apparent by the following preferred embodiment in conjunction with the accompanying figure. This application is in the field of medicine, which is the preferred field of application of the present invention.
In the course of this, security measures which singly are as such already known and which all ensure highly secure data transmission in the mentioned field of application, are explained and executed in combination with the invented device and process. It is a matter of course, that the combinations of single security measures described in the following are independent of each other so that omitting one of these steps or replacing it by other known security measures is also feasible.

The present example relates to the electronic transmission of medical data over public networks. The security measures used to do this ensure the best possible protection of these sensitive data. In this area, a typical process begins in the office of the doctor of a patient. The physician transfers the patient to a specialized doctor who the physician does not know at this point in time because the patient has the right of free choice. Hitherto, the patient was usually given a sealed envelope containing the important medical data and the transfer slip which he was to give the specialized doctor of his choice.
If the physician wanted to transmit the data to the colleague electronically, he would have had to know the colleague's identity at the time of the transfer. This is no longer necessary with the process described in the following using the invented device and the invented method. The basic system

comprises at least one central data station, a server, to which a connection can be set up from the data stations participating in the system. In the present case, the data stations are the doctors' external computers. In the described instance, this means the transferring doctor files the patient's required medical data in the server for the (still unknown) colleague and this colleague can retrieve these data from the server at a later date.

The description of the security mechanism starts with the general security aspects of the design of the system and then explains the general and the specific use of the cryptographic process and finally the integration and technical realization of the invented device.

Any form of active reading of data requires, if need be limited, access authority to the data station where the data are stored. In the present example, the system does not permit reading access to the server but only the transmission of a data request through the participating sites. Upon verification of the authority to receive, the data are sent to the requester, in the present case the specialized doctor requesting the data, thereby preventing as far as possible direct access to the data content of the server from an external site.

For communication, the exemplary concept employs a type of communication known as “remote procedure call” (RPC), wherein a request to carry out a certain function and to send back the result of this function is transmitted to the server from an external computer. The advantage of this type of communication is that running on the server is a problem-specific application which executes solely those operations provided in the system function. In this manner, functions that go beyond this, e.g. direct access to the data, are ruled out with absolute certainty.

Furthermore, the concept also provides that in order for a network participant to set up a connection, the network participant first sends a request to set up a connection to the server. This operation itself does not set up a connection. But rather, it is provided that this request is realized as so-called "D channel information". This is a special ISDN network function in which prior to "accepting" a call, thus free of charge, only the identifier respectively the number of the caller is transmitted. Subsequently, the server checks whether the number matches one in the list of participants stored in the server. Only if the transmitted caller's number is one belonging to an "authorized" network participant, will the server initiate a return call via a number stored in an internal data bank.
The special security aspect of this solution is that although the caller's number transmitted in the D channel can, in certain circumstances, be falsified (can be "masked"), the connection via the server is set up in any event with the actual holder of this number, thus the authorized network participant. Therefore, in the worst case, a connection is initiated to a network participant who did not request it but belongs to the authorized group. In any case, no transmission of data occurs, because being unable to provide a data request, the computer of the participant who was called back without requesting the data is unable to set up a connection.

The described exemplary concept is based on transmitting documents once in the sense of "mailing". As soon as a document is requested from the server by an authorized addressee and it is sent to him, it is erased in the server (first logically and then physically). This is particularly possible with the present application, because the data are only intended for one addressee.
If the data are to be accessible to several addressees, this measure is not provided.
Moreover, all the data are provided with an expiration date. When it has expired, the data are also erased physically. In this

manner, data do not accumulate in the server, thus making it impossible to link different documents relating to one patient or to one doctor. The identification of the documents occurs via a procedure ID granted only once for this specific communication procedure and does not permit drawing any conclusions about the patient. The requesting doctor must know this ID, and it is preferably given to him with the respective paper document (transfer slip) by the patient himself.

In addition to the described security measures, all the data are encoded and signed for the transmission and storage utilizing standard cryptographic processes with a secure exchange of keys, for example corresponding to X.509. These are symmetric encoding processes such as triple DES, "blowfish" or IDEA for encoding large amounts of data and asymmetrical encoding processes such as RSA or elliptical encoding processes for the digital signature (encoding a hash value) and the encoding of the symmetrical session key.

In order to secure the authenticity and the integrity of the transmitted data, each document is signed before transmission with the sender's private key, in the present case the transferring doctor's. For this purpose a hash value is determined which is asymmetrically encoded with the sender's private key. The signature of the document is preserved even after decoding (see following steps) and thus is at disposal for forensic relevant verification of the authenticity of the document. However, a prerequisite for the proof of authenticity is that the document is stored in the signed form at the recipient, if need be also an unsigned version is stored there in addition to the readable one. Separate storage of the document and the signature is possible. However, it has the danger that unintended modification of the document, e.g. when opening the word processing system, invalidates the signature. Archiving the document is the recipient's responsibility.

The single documents are symmetrically encoded using a random generating key (session key) with a length of N (for security reasons N should be larger than or equal 128). The session key employed for encoding is encoded with the server's public key, i.e. the invented device installed in the server. For security reasons, the length of the key should be at least 1024 bits.

As the document including the signature are encoded, the server cannot check the authenticity of a document, neither with regard to its error-free transmission nor its existence per se (electronic "registration"), without decoding the data. In order to permit this, the signed and encoded document is signed again in addition.

The document prepared in the aforedescribed manner is processed as a MIME-compatible file and transmitted in this form to the server by means of a corresponding RPC. In the server, the document is unpacked out of the MIME format and the external signature is checked and removed in the process. In this manner, its intactness, i.e. the completeness and authenticity of the document, is checked and then logged. After successful filing of the (encoded) document, a receipt signed with the server's personal key is returned to the sender by the server as infallible proof of successful filing of the document.

The to-be-forwarded document is stored in the server in the (internally) signed and then encoded form. No one can decode it in this coded form.
An accompanying not coded procedure ID, which is part of each procedure, serves as filing respectively access criterium for administering the coded documents. As already explained in the preceding, this procedure ID is given later by the patient directly to the doctor of his choice. This ID is clear to the server from the transmitted request for data of which it is a part.

Data can be requested by participants of the respective network by providing this respective procedure ID, their ISDN number and their doctors's identifier.
Additional identifiers, e.g. for distinguishing the respective patient, may be required to increase security further.

When the respective specialist doctor requests data, the invented device recodes the data in such a manner that it becomes readable for the requesting doctor. For this purpose, the session key employed for symmetrically encoding the data is decoded with the server's private key present in the server and immediately recoded with the requesting recipient's public key. This public key is, along with the doctor's ID and the ISDN number, stored in the list of participating network doctors and can be updated via the service of a participating trust center.
It is not necessary to decode the medical data itself. In order to later decode the data, only the session key, now readable for the recipient, has to be known which was randomly generated in the course of encoding.
In this manner, it is impossible that the medical data themselves are present in the server in an uncoded form at any time. There is no access to the coded data during recoding. Processed is solely the session key used for their encoding and which is "recoded" from a form only readable for the server into a form readable for the requester.

The document encoded for transmission to the recipient is signed again to secure correct transmission to the recipient and to secure possibly desired logging, notably by the server with its personal key.

The document prepared in the manner described in the preceding is processed as a MIME compatible file and is sent in this form as a RPC reply to the data request to the requester.

At the recipient the document is unpacked out of the MIME format, the external signature is checked and in the process removed. In this manner, the intactness, i.e. the completeness and the authenticity, of the document is checked again. The recipient's receipt signed with his personal key is returned to the server as infallible proof of successful transmission of the document.

The recipient can decode the coded session key with his personal key and then decode the data themselves with it. Following this, the data are present only in the form that is readable with the sender's signature.

The purpose of the signature of the initial document is to be able to prove the docucent's authenticity. In order to preserve the signature, it is necessary to store the document in the signed form.

A possible vulnerable point is the server's private key. As all the stored data, more precisely all the session keys of the stored data, can be read with the same server's key, it would pay, in particular, to attack this key and, on the other hand, an attack is facilitated by the amount of data present.
In order to take precautions against this circumstance, in a preferred embodiment of the present invention, as an additional security mechanism, it is provided that the session key is split in two.

As described in the preceding, the original data is encoded with a N-bit (N being preferably greater than or equaling 128 bits) symmetrical key. This key is usually asymmetrical for transmission and only encoded in a manner that is readable to the recipient. Decoding, even forcible decoding, the session key thus suffices to be able to decode the data itself.

In order to prevent this, the following modification is introduced. In this modification, the session key is split in two before its symmetrical encoding. For instance, M ($0 < M < N$) of the N bits of the session key are removed as a so-called "procedure key". Only the remaining ($N-M$) bits of the session keys are asymmetrically encoded and transmitted along with the data.
Recoding the data with the reduced session key occurs in the same manner as described in the preceding in connection with a whole session key. As the data themselves never have to be decoded there, the whole session key is not required. Only the rudimentary session key is decoded by the server and encoded again for the requester.

Decoding at the recipient differs from the aforedescribed procedure in that after decoding of the session key by means of the recipient's private key, this session key has to be expanded by the M bits of the procedure key separated at the sender. Following this, decoding can occur as described in the preceding.

The procedure key generated at the sender of the data, i.e. the separated M bits, are added to the procedure ID which was also generated there. A combination of the procedure ID and the procedure key yields the so-called procedure identifier which is printed on the accompanying paper document (transfer slip, prescription, ...) and read at the recipient. The procedure key contained in the procedure identifier is never transmitted to the server so that all the information required to actually decode a document never comes together in the server.

Figure 1 shows an example of the invented device as utilized for carrying out the preceding application example.
The device is preferably designed in the form of a plug-in module 1 (recoding module) for modular installation in the server. In the present case, module 1 contains a chipcard 2 which conducts the decoding of the coded session key 10a with the aid of the

server's private key stored in the chipcard 2 and the recoding of the session key with the public key of the addressees respectively the requesters of the data. The server's private key is not accessible from outside the chipcard respectively from outside the module. The requester's public key is conveyed to device 1, as is the to-be-recoded session key 10a, via an interface provided for this purpose. The recoded session key 10b is issued via a further interface.

The server's processor itself assumes the task of separating the session key 10a from the coded data block 11, conveying it to device 1 and adding the session key 10b supplied and recoded by the device to data block 11 again, as the diagram in the figure shows.

However, this separation and renewed combination can also be conducted directly in device 1. In this case, the entire data block 11 with the session key 10a would have to be conveyed to the device.

The server's personal key is undoubtedly a critical point with regard to intentional, unauthorized attempts to gain access to the data.

Usually keys must not respectively should not be stored in the computer on which the coded data are stored respectively are processed. However, if the server operates automatically as in the present case this is unavoidable. For this reason, in the present embodiment the device is designed as a sealed, encapsulated unit that is able to carry out the entire procedure of recoding the data internally without the decoded (even rudimentary) session key or even only traces of its decoding leaving the autonomous unit.

Today there are already key cards available on the market that are able to carry out the asymmetrical encoding of a 128-bit session key according to a 1024-bit RSA process completely on the chip of the card. Soon such cards will also be available for 2048-bit keys.

In particular, there is the possibility to have the two keys (public key - private key) generated directly on the card or in a lawful, certified trust center without the private key of the card ever leaving the card. Such a key card can be utilized in the invented device as chipcard 2. In a first step, the coded session key 10a is conveyed to this chipcard 2. This coded session key 10a is then decoded with the aid of the card's private key, which in the preceding was referred to as the server's private key. The decoded session key is issued by card 2 without, however, ever leaving device 1. But rather in a second step of card 2, it is entered again, this time along with the addressee's public key. In this second step, card 2 returns the recoded session key 10b. This is shown by arrows inside device 1 in the figure. The additional circuit, buffer unit 4, required for this serves, i.a. to coordinate these procedures temporally. This buffer unit 4 can, for example, be realized by a suited, programmed micro the coded session key 10a processor or by means of a logic circuit.

In order to prevent drawing conclusions about the internal procedures from the modulations on the current supply of the device, in the present embodiment of the device, a constant current circuit 3 is provided which ensures within the scope of a defined interval of the supply voltage that the device is provided with a constant and modulation-free current input. When exceeding or falling short of certain limits of the operating voltage or other operation parameters, such as, e.g. temperature, the device turns off with an error message.

As conclusions can also be drawn about the internal procedures from the temporal behavior of the device, all the input data can be first buffered in the buffer unit 4 or in a special unit provided for this purpose and the results can be issued after always the same time regardless of how much time the internal procedures took.

"Bugging" the electronic procedures in the device is prevented in the present embodiment by an electromagnetic screening 5 of the device.

Provided as the interface of the device is, on the one hand, an interface for the input of the asymmetrically encoded session key 10a (respectively a rudiment of this key) and of the public key of the requesting recipient. On the other hand, an interface must be provided for the output of the asymmetrically encoded session key 10b (respectively its rudiment). Both interfaces can be physically identical with a suited design.
Furthermore, for generating respectively checking signatures, interfaces can be provided for the input of the hash value of the to-be signed document and for the output of the symmetrically encoded hash value, i.e. the signature.

Although the aforedescribed measures were presented in the context of the example on which the present invention is based, this idea and the invented device can, of course, also be applied in other fields requiring secure transmission of data between two data stations via intermediate storage on a server.

Furthermore, the present invention is not limited to the transmission of data only via one intermediate station respectively one server. The data can also be transmitted via multiple servers, with the data request being executed by another server always in the same manner as the request by an addressee. Then the data are treated in the other server in the same manner as in the first server, i.e. this other server must also be provided with the invented device.

What is Claimed Is:

1. A device for secure transmission respectively forwarding of coded data via a data station of a network, having
- an input unit for receiving said coded data (10a) and an external key;
- a unit (2) for decoding said coded data with an internal key and recoding said data with said external key, with said internal key not being accessible from outside said device; and
- an output unit for issuing said data (10b) encoded with said external key.

2. A device according to claim 1,
wherein said internal key is stored on a suited data carrier inside said unit (2) for decoding and encoding.

3. A device according to claim 1 or 2,
wherein said unit (2) for decoding and encoding comprises a chip card as said carrier of said internal key.

4. A device according to claim 1 or 2,
wherein said unit (2) for decoding and encoding comprises an active chip card with an integrated processor, which partly or completely assumes the decoding and encoding of said data.

5. A device according to one of the claims 1 to 4,
wherein said device is provided with a buffer and logic unit (4) for temporal control of the data flow in said device, said buffer and logic unit (4) first conveys said coded data (10a) for decoding to said unit (2) for decoding and encoding and receives said data back decoded, and said buffer and logic unit (4) subsequently conveys said decoded data for encoding with said external key to said unit (2) for decoding and encoding and receives it back as coded data (10b).

6. A device according to one of the claims 1 to 5, wherein said input unit and said output unit are provided with standard interfaces for the input and output of said data.

7. A device according to one of the claims 1 to 6, wherein said unit (2) for encoding and decoding utilizes asymmetrical encoding processes.

8. A device according to one of the claims 1 to 7, wherein said device is provided with a complete mechanical and electromagnetic encapsulation (5) and with a possibility of sealing.

9. A device according to one of the claims 1 to 8, wherein a buffer unit is provided which buffers all the data flows inside said device to compensate for possible internal-key-dependent processing times so that the data output of said device occurs according to a process-independent time span.

10. A device according to one of the claims 1 to 9, wherein a unit (3) is provided for buffering the current input of said device in such a manner that said current input of said device is independent of the current input of said unit (2) for decoding and encoding, which is dependent on said internal key, or of other internal circuits.

11. A device according to one of the claims 1 to 10, which is further provided with a unit for receiving a first data block containing said coded data (10a) in addition to further data (11) and for separating said coded data (10a) from said further data (11) and with a unit for joining said further data (11) with the recoded data (10b) to a second data block and for the output of said second data block, with said encoded data representing a key with which said further data (11) are encoded.

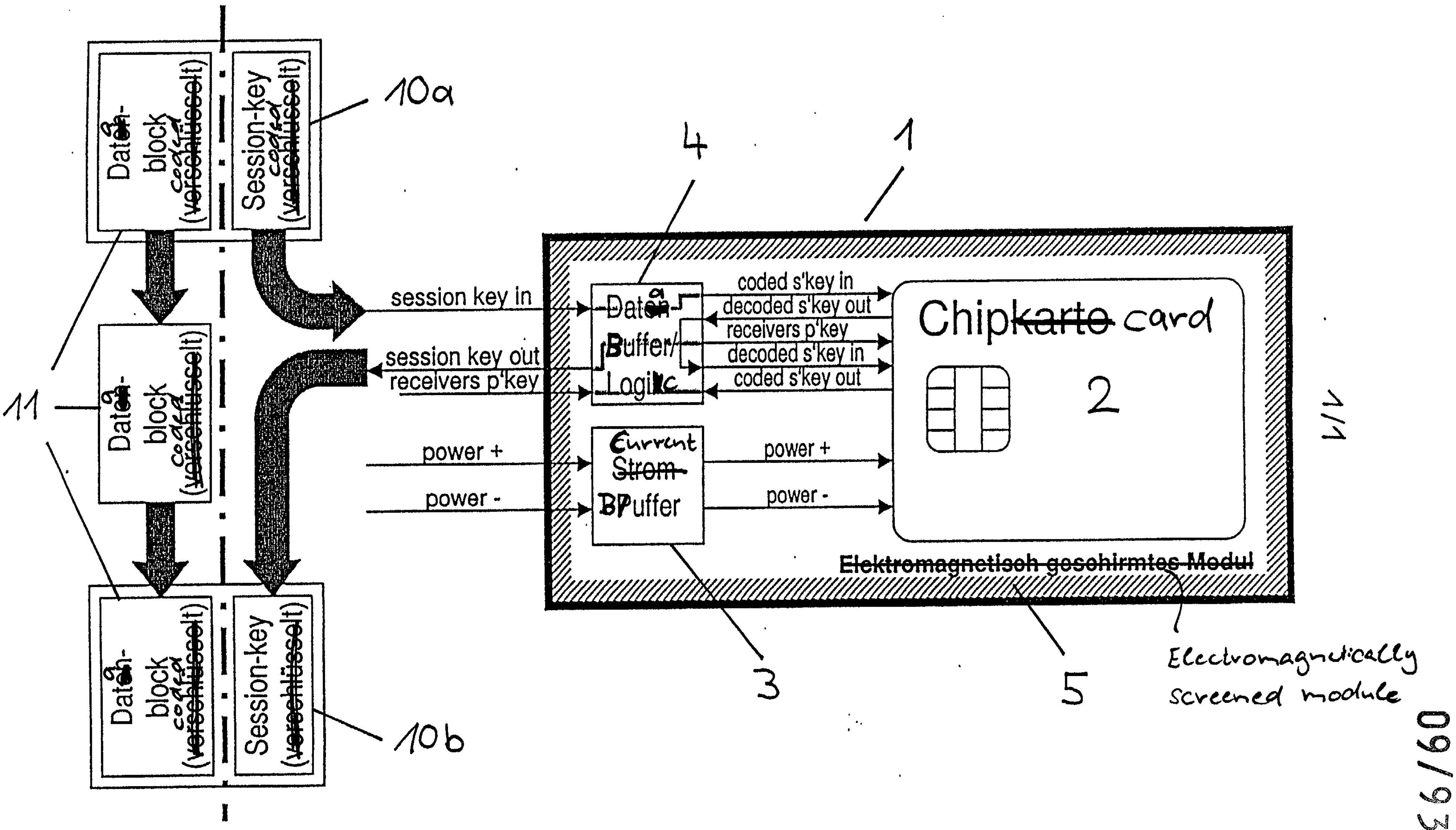
12. A process for secure data transmission from a first data station via a second data station to a third data station using the device according to one of the preceding claims, having the following steps:
- encoding of the data in said first data station with a first key;
- encoding of at least a part of said first key in said first data station with a public key of said second data station;
- transmission of said coded data (11) together with the coded part of said first key (10a) to said second data station;
- storage of said coded data (11) and of said coded part of said first key (10a) in said second data station;
- request of said data by said third data station;
- decoding of said coded part of said first key with a private key of said second data station matching said public key and recoding of the previously decoded part of said first key with a public key of said third data station; and
- transmission of said coded data (11) together with said recoded part of said first key (10b) to said third data station.

13. A process according to claim 12, whereby said first key is completely encoded and transmitted.

14. A process according to claim 12, whereby only a part of said first key is encoded and transmitted to said second data station.

15. A process according to one of the claims 12 to 14, whereby said coded part of said first key is decoded in said third data station with said private key of said third station and subsequently said data (11) are decoded with said first key.

16. A process according to one of the claims 12 to 15, whereby said public key of said third data station is taken from an internal data bank of said second data station or is determined by consultation with a trust center.


~~Daten~~ Data-
block
~~(verschlüsselt)~~ coded
Session-key
~~(verschlüsselt)~~ coded
10a
11
10b
4
1
session key in
session key out
receivers p'key
power +
power -
~~Daten~~ Data
~~Buffer~~ Buffer/
~~Logik~~ Logic
~~Strom~~ Current
~~BP~~ Puffer
coded s'key in
decoded s'key out
receivers p'key
decoded s'key in
coded s'key out
power +
power -
~~Chipkarte~~ Chip card
2
~~Elektromagnetisch geschirmtes Modul~~
Electromagnetically screened module
3
5

09/937819

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

Docket No. 5551

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled DEVICE AND METHOD FOR SECURE ELECTRONIC DATA TRANSMISSION, the specification of which is attached hereto unless the following box is checked:

[X] was filed on January 20, 2000 as United States Application Number or PCT International Application Number PCT/DE00/000189 and was amended on April 25, 2001 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed
PCT/DE00/000189 (Number)	PCT (Country)	20 January 2000 (Day/Month/Year Filed)	Yes [X] No [ ]
199 14 225.4 (Number)	Germany (Country)	29 March 1999 (Day/Month/Year Filed)	Yes [X] No [ ]
(Number)	(Country)	(Day/Month/Year Filed)	Yes [ ] No [ ]

COMBINED DECLARATION & POWER OF ATTORNEY Docket No. 5551

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

(Application Number) (Filing Date)

(Application Number) (Filing Date)

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application No.) **(Filing Date)** **(Status-patented, pending, abandoned)**

(Application No.) **(Filing Date)** **(Status-patented, pending, abandoned)**

I (we) hereby appoint the following attorney with full power of substitution to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

4

ALFRED W. BREINER, Reg. No. 18,676; THEODORE A. BREINER, Reg. No. ~~32,103;~~ MARY J. BREINER, Reg. No. 33,161; and C. BRANDON BROWNING, Reg. No. 44,570.

Address all correspondence to -

BREINER & BREINER, 115 North Henry Street
P.O. Box 19290, Alexandria, Virginia 22320-0290

Address all telephone calls to -

Mary J. Breiner at (703) 684-6885

COMBINED DECLARATION & POWER OF ATTORNEY Docket No. 5551

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1-6C

Full Name of Sole or First Inventor:
(given name, family name) Volker PAUL

Inventor's Signature Volker Paul Date 08-Oct. 2001

Residence: St. Ingbert, Germany Citizenship: German

Mailing Address: A.-Weisgerber-Allee 144,
D-66386 St. Ingbert, Germany

2-6C

Full Name of Second Joint Inventor, if any
(given name, family name) Bertram BRESSER

Inventor's Signature Date 11-Oct.-2001

Residence: Dillingen, Germany Citizenship: German

Mailing Address: Augrät 32, D-66763 Dillingen, Germany

Full Name of Third Joint Inventor, if any
(given name, family name) ____

Inventor's Signature ____ Date ____

Residence: ____ Citizenship: ____

Mailing Address: ____
